Exploiting Vehicles' Reputation to Mitigate DoS Attack

Gianpiero Costantino, Fabio Martinelli and Ilaria Matteucci
Istituto di Informatica e Telematica, CNR, Via G. Moruzzi, 1, Pisa, Italy

Keywords: Security and Safety in Automotive, Connected Vehicles, Reputation, DoS Attack.

Abstract: Recently the convergence of safety and security needs in automotive systems is one of the main challenges of the research community. However, the different nature of safety and security metrics suggests that no individual assessment technique is sufficient, in isolation, to validate large systems that are intended to be both safe and secure. The introduction of new generation ICT systems into vehicles makes them potentially vulnerable to security attacks that may impact on the safety of passengers, pedestrians, and vehicle itself. Hence, entities involved in a communication have to be evaluated trustable by means of specific mechanisms of the vehicle or infrastructure system. This work aims at proposing an algorithm for the calculation of reputation of vehicles in a Vehicular Ad Hoc Network (VANET) based on the type and number of exchanged messages. The ultimate goal is to mitigate the Denial of Service (DoS) attack in such kind of communication by acting as a firewall with respect to not trustable vehicles. Indeed, the DoS is a security attack that affects the availability of network bandwidth. This may have an impact on safety of drivers and vehicles since it may prevent the communication and spread of important information for, e.g., human life.

1 INTRODUCTION

Nowadays, the more and more pervasive usage of ICT in automotive ecosystem is raising the need to consider security issues related to cars, trucks, and motorbikes. In the last 5 years, both car manufacturers and academics have performed studies in the field of automotive cyber-security to identify a detailed list of threats that can be exploited by attackers. This research has provided a set of recommendations to car manufacturers to overcome the found threats. Based on inputs from the Automotive Cyber Security Thought Leadership event (held in November 2014), the Institution of Engineering and Technology (IET) has been recently published a report (IET, The Institution of Engineering and Technology, 2014) on automotive cyber-security issues. IET provides some recommendations to address such issues to ensure that future connected vehicles be safe and more efficient.

New technologies make vehicles connected and users able to interact with own vehicles through mobile devices. These new opportunities represent an advantage in terms of connectivity, revenue, and safety but they have also some drawbacks in terms of security. The main issues are mostly related to security *CIA* triad, i.e., Confidentiality, Integrity, and Availability. In automotive systems, *Confidentiality* is intended related to exchange of information between the user mobile device and the vehicle. The exchanged data may be confidential and must not be stolen by an untrusted party. *Integrity* means that shared data or information are not modified or altered by another entity different from the source. In automotive, this can be violated through applications able to interact with the vehicle system. The same for the information (requests, data, etc.) exchanged between the mobile device and the connectivity system that might be misinterpreted and cause failure in control units. Thus, a hacker may use these vulnerabilities to get internal data of the vehicle or try to acquire control of parts of the car. *Availability* is a guarantee of reliable access to the information by authorized people. In automotive systems, it is mostly related to communication services that have to guarantee the correct flow of information, such as traffic information, safe alerts, and so on, among circulating vehicles.

In this paper we focus on *vehicle-to-infrastructure* (V2X for short) and on *vehicle-to-vehicle* (V2V for short) communications. Both of them are subjects to several security attacks, and among others, one of the most common is the attack on network availability also referred as *Denial of Service* (DoS) attack (Razzaque et al., 2013). The DoS attack is an attempt to make a communication network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of vehicles con-

Costantino, G., Martinelli, F. and Matteucci, I.
Exploiting Vehicles' Reputation to Mitigate DoS Attack.
DOI: 10.5220/0005844500750082
In *Proceedings of the International Workshop on domAin specific Model-based AppRoaches to vErificaTion and validaTiOn (AMARETTO 2016)*, pages 75-82
ISBN: 978-989-758-166-3

nected with other vehicles or with the infrastructure. Moreover, DoS is a very common attack where the attacker can overpower a vehicles resources or jam the communication channel used by the Vehicular Ad Hoc Networks (VANET) to bring down the VANET itself or even cause an accident with a damage of safety drivers.

We consider that both V2X and V2V communications mainly happen through a VANET, that is a specific type of *Mobile Ad Hoc Network* (MANET) providing communications between nearby vehicles and roadside equipment. A MANET is a structure composed only by wireless nodes, without any fixed devices, that is set up instantly, as soon as devices, which do not even know each other, are available. A MANET survives until the participants remain linked together. Similarly, vehicles of a VANET are considered communication nodes able to belong to a self-organized network without any prior knowledge of the presence or identity of the others.

Starting from these considerations, we propose an algorithm to calculate the reputation of vehicles while they are circulating on road. Our algorithm is based on the direct observation of the messages generated and forwarded by vehicles. These pieces of information are collected and sent to a central entity that is able to establish the reputation of each vehicle. So, established reputation values are sent back to the vehicles to notify them about their current behaviours. This approach helps vehicles to detect the occurrence of an anomalous behaviour with respect to a possible DoS attack, and intrinsically the presence of a malicious entity in the network. Finally, our algorithm tries to validate the communications by providing a way for isolating the attacker.

The paper is organized as follows: Section 2 provides some background notions about Vehicle Ad Hoc Network. Section 3 describes the reference scenario we use in the paper to exemplify the proposed approach. Section 4 introduces the technique used to calculate the reputation of vehicles, to verify the behaviour of a vehicle and, eventually, to isolate it whether considered as malicious. Section 5 discusses the related work on security issues in automotive systems with a particular eye to security aspects of VANET. Finally, Section 6 draws the conclusion and proposes some possible for future work.

2 VEHICULAR AD HOC NETWORKS IN A NUTSHELL

A modern vehicle can be considered as a network of sensors/actuators on wheels. VANET is a special kind of Mobile Ad-hoc Network (MANET) where vehicles equipped with the technologies are the key constituents. According to (Razzaque et al., 2013) a VANET differs from a MANET in several aspects: i) Large scale, potentially billion of vehicles, ii) Fleeting contact with other vehicles, iii) Nodes not as constrained in terms of energy, storage, and computation, iv) Higher mobility, and v) Privacy requirements.

One of the main objective of a VANET is to allow communication between vehicles on the roads and their environments with the aim of improving the safety of drivers. To this aim, each vehicle belonging to a VANET needs to have an OBU (On-Board Unit), which is a communication device mounted on vehicles, and a Wireless Sensor Network (WSN) supported roadside unit (RSU).

By using OBUs, vehicles can be connected with other vehicles as well as with the roadside unit. The RSU is also connected with the backbone network, e.g., the roadside infrastructure, in such a way that it can communicate with many other network applications and services, including the Internet access, which can be provided to the vehicles (Qian and Moayeri, 2008).

To improve the functionalities and capabilities of VANET, multiple ad-hoc networking technologies have been integrated on them, such as WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, and ZigBee. These technologies make more easy, accurate, effective, and simple all communication between vehicles. Furthermore, the IEEE 1609 (P1609.2) explicitly defines security aspects such as secure message formatting, processing, and message exchange to put in evidence their impact on vehicle safety aspects.

VANETs are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC). Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Thus, VANETs are envisioned as the most important entity of the Intelligent Transportation Systems (ITS).

The main security issues of V2X communication mainly concerns security issues peculiar of WiFi connection. Indeed, in (Chou et al., 2009) the authors state that, even though V2V and V2X are both wireless mobile networks, they are different and participate in vehicular network with different communication modalities. For that reason, they propose WiMAX instead of WiFi for V2X infrastructure. They focus on a static setting in urban environment and describe some measurements by showing that WiMAX technology provides a longer communication range and, for applications like file downloading, one might want to use a larger frame size to have a better throughput. The setting of frame size has a strong impact on performance of WiMAX.

Hereafter we focus on the DoS security attack within V2V communications, how it can impact on safety aspects, and we provide a possible solution for mitigating the attack. As we will see in the next section, our approach works at application level so it is independent from the used physical technology.

3 REFERENCE SCENARIO

As reference scenario, we consider a vehicular network in which all vehicles are connected with the roadside infrastructure exploiting the WiMAX technology. Vehicles communicate with each other by exploiting the OBU technology. Like any other networks, also these communications are affected upon the Denial of Service (DoS) attack. The DoS is an active and malicious attack in nature. For instance, if a malicious adversary wants to create a massive pileup on the highway, he could exploit an accident and then use a DoS attack to prevent the dissemination of warnings to other drivers.

The reference scenario is the one graphically depicted in Figure 1. Let us consider two vehicles both circulating on a sector of a roadway. Let us also assume the presence of a traffic jam some miles ahead. Vehicles belonging to the VANET of that sector of the roadway start to communicate each other to spread the information as much as possible. Receiving this kind of information on time increases the safety of drivers. Indeed, according to (Wang and Thompson, 1997), about 60% roadway collisions could be avoided if the driver was provided warning at least one-half second prior to a collision.

3.1 Modelling the Vehicles' Behaviour

Vehicles that travel in a distributed environment can assume several behaviours that may depend on different reasons. A vehicle may decide to be fully collaborative and to constantly participate in the V2V communications. On the other side, a vehicle can decide to assume a dishonest behaviour and to deny V2V communications by dropping messages it receives, *Black hole* attack (Deng et al., 2002).

According to the BUG threat model (Bella et al., 2005), an attacker can assume three different states of behaviour that we recast when the goal is reputation:

- *Bad:* when the vehicle is essentially selfish, and damages the network intentionally by neglecting or limiting particular communications;
- *Ugly:* when the vehicle essentially assumes an opportunist behaviour according to its cost/benefit analysis of the context.
- *Good:* when the vehicle uses its resources to provide V2V communications nodes without any direct interest.

4 UNDERSTANDING THE VEHICLES' BEHAVIOUR

In this section we present our technique to calculate the reputation of vehicles, and to isolate those one that are suspected to be attackers. We consider the reputation as main information to understand the behaviour of vehicles, and more specifically, it is used as parameter to identify malicious vehicles. Indeed, reputation is calculate in accordance to a *principle of collaboration*: vehicles in a VANET work in an open net and their collaboration is the sole mean to allow communications and the survival of the VANET itself (Bella et al., 2008).

In the algorithm we propose, vehicles are able to observe the behaviour of other vehicles that they meet during the journey. The algorithm is composed of four steps: as a first step, each vehicle performs a *direct observation* of neighbours and evaluates their behaviour by comparing the number of messages they *generate* and *forward*. Indeed, a trustworthy vehicles has a collaborative behaviour and forwards messages as much as possible to allow the information is circulated and distributed uniformly over the network. Then (second step), at fixed time, each vehicle transmits the collected values to a central server belonging to the roadside infrastructure by using V2X communications. In particular, a *central server* of the roadside infrastructure acts as a collector of all local observations done by vehicles. As third step, the central server calculates a single value of reputation for each vehicle that is travelling in the considered roadway. Finally, in the fourth step, the complete set of reputation values is sent to all vehicles that will receive updated reputation values of other vehicles they are able to communicate with.

The main goal of the proposed algorithm is to provide a method of vehicles to rapidly identify and eventually isolate malicious vehicle. It is designed to detect and overcome DoS attacks. Consequently, it allows drivers to improve traffic safety and road efficiency. Furthermore, by guaranteeing the availability of communications network and road efficiency, it leads to a reduction of pollution, thus positively impacting on the environment.

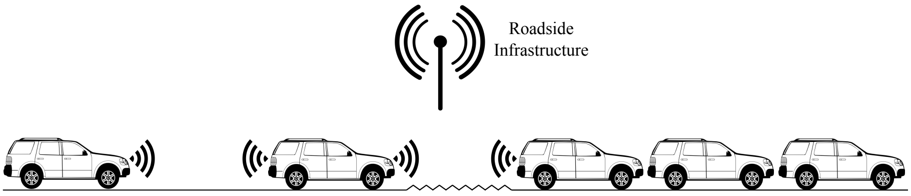

Figure 1: A graphical representation of the reference scenario.

4.1 Direct Observation

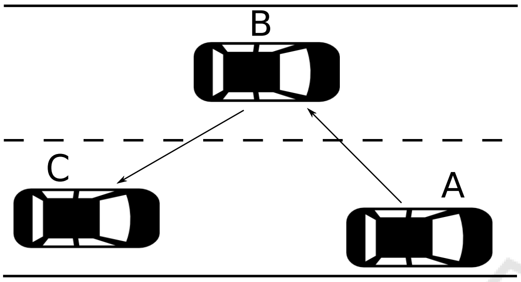

Figure 2: A graphical representation of V2V communications.

In Figure 2 we show an example of communications among three vehicles. Vehicle *A* generates a message and sends it to vehicle *B*. When, *B* receives the message, it propagates the message to *C* and so on. Basically, according to this propagation mechanism, *B* and *C* vehicles are able to locate the vehicle that generated the message by observing the packet structure. In particular, *B* understands that *A* generated the message, and *C* understands that the message was only forwarded by *B* but not generated.

We call *Direct Observation* the phase in which a vehicle calculates the number of packets generated and forwarded by *close* vehicles. Vehicles are considered close when the distance between them is only a single hop. So, when a vehicle receives a message, it checks whether such a message has been generated or forwarded by the close car. This information is stored into a local table that we call *Vehicles Local Observation* (VLO).

Table 1: Example of Vehicles Local Observation Table.

V_c	G_m	F_m
B	19	5
G	5	16
...	...	...
P	12	40

An example of VLO calculated by *C* is illustrated in the Table 1, where, V_c says that the table belongs to vehicle *C*, while G_m and F_m show the number of Generated and Forwarded messages of met vehicles, such us *B*, *G*, *P*, and others. Note that each vehicle can be uniquely identified by the other, for instance, through its license plate.

4.2 Collecting the VLO Tables

Once VLO tables are populated and updated, each vehicle sends its VLO to the central server that belongs to the motorway infrastructure. Such communications exploit V2X connections. We assume that, at fixed time, for instance every *5* minutes[1], vehicles send their VLO tables to the server, which collects them. We point out that communications with the server are not performed all at the same time, but they depend on the moment when a vehicles entered in the roadway sector under observation.

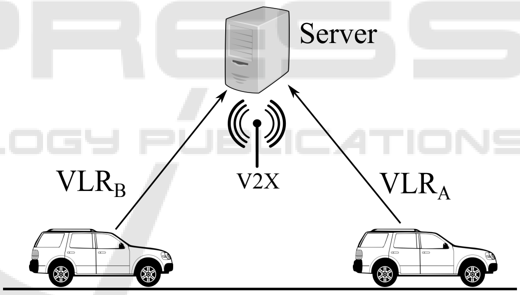

Figure 3: Sending VLOs to the central server.

In Figure 3 we pictorially show the phase in which cars share their VLO with the server. When, the server receives VLOs, it populates its table that contains all G_m and F_m aggregated for each vehicle. We call this table *Vehicles Global Observation* (VGO), and in Table 2, we illustrate the VGO that contains the aggregated values of G_m and F_m of each vehicle circulating on the considered sector.

The strategy to populate the VGO table works in the following way. If the server receives a VLO that contains a new vehicle identity, i.e., information about a vehicle that is not already present in the VGO, the server just creates a new entry in the table and appends its values of G_m and F_m. On the contrary, if the server has already values of G_m and F_m for certain

[1] Note that this is an approximate value that should be fixed only after performing accurate simulations.

Table 2: Example of Vehicles Global Observation Table.

V	G_m	F_m
B	1509	150
G	501	1654
...	...	...
P	350	467

vehicles contained in the VLO, then it updates those values in the following way:

$$G^j_{m_{new}} = G^j_{m_{old}} + G^j_{m_{rcv}} \tag{1}$$

where $G^j_{m_{old}}$ represents the number of messages generated stored in the VGO for the vehicle j, $G^j_{m_{rcv}}$ represents the number of messages generated stored into the VLO for the vehicle j, and $G^j_{m_{new}}$ is the new value for the number of messages generated by j.

The same approach is also applied to calculate the aggregated values of messages for vehicle j to store in the VGO. So, the formula is the following:

$$F^j_{m_{new}} = F^j_{m_{old}} + F^j_{m_{rcv}} \tag{2}$$

where $F^j_{m_{old}}$ is the value of forwarded messages stored in the VGO, $F^j_{m_{rcv}}$ is the number of forwarded messages calculated locally, and $F^j_{m_{new}}$ represents the aggregation of the previous two values.

4.3 Vehicles' Reputation

As we presented above, the VGO contains an overall observation of the behaviour of each vehicle travelling in the roadway. Such a behaviour expresses the reputation taken by the vehicle up to the moment it has been established. According to the principle of collaboration, the reputation of each vehicle is calculated as the ratio of F_m and $F_m + G_m$. The formula that calculates the reputation of a generic vehicle j is:

$$Rep^j = \frac{F^j_m}{F^j_m + G^j_m} \tag{3}$$

Let F^j_m and G^j_m the aggregated values of forwarded and generated messages of the vehicle j stored in the VGO. It is worth noting that the result of Equation 3 is normalized to obtain value in the interval between 0 and 1. Thus, the structure of the VGO table is updated as we show in Table 3:

Table 3: Vehicles Global Observation Table with Reputation Values.

V	G_m	F_m	Rep.
B	1509	150	0.09
G	501	1654	0.77
...	...	...	...
P	350	467	0.57

The VGO table with the reputation value of each car basically shows the behaviour taken by cars in the motorway. More specifically, we say that a $Rep^j \leq 0.3$ is an indication of an anomalous and bad behaviour, for instance a *DoS* attack. On the contrary, $Rep^j \geq 0.7$ indicates a collaborative and also good behaviour.

Note that, even thought the reputation is calculated considering both newer and older message, our reputation algorithm does not imply that a malicious vehicle will be always tagged as malicious. In fact, by reverting to a collaborative behaviour, that vehicle will improve its reputation.

Remark. The proposed calculation is intended to not be optimal in general. Our aim is to mitigate the DoS attack by monitoring the number of messages that are input on the considered network. The proposed algorithm can be refined to better estimate the reputation of a vehicle. So, it may exploit additional parameters that may help to mitigate security issues related to data-integrity and privacy of exchanged messages.

4.4 Broadcating the VGO Table

In this last step, the central server is in charge of notifying the vehicles with the reputation values available in the VGO. Here, vehicles receive the VGO and use the reputation values as indication of the behaviour of the cars.

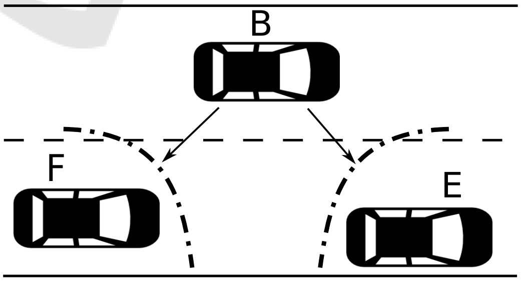

Figure 4: Isolation strategy against DoS attack.

In Figure 4 we show an attempt of DoS attack performed by vehicle B. This car continuously generates messages that may flood the V2V communications. Nevertheless, vehicles E and F already know the behaviour of B because they checked the VGO table. So, when E and F receive messages from B, they may decide to isolate B by dropping the messages generated by it. This approach is close to that one applied by firewalls when they detect a *DoS* or *bruteforce* attack. In the same fashion, here vehicles may decide to isolate the "spammer vehicle".

However, it may happen that the vehicle, which is considered an attacker, may also generate an alarm message that should not be dropped by its neighbours. In this situation, we foresee that vehicles close to the attacker do not directly drop the packet, but before they check the content, for instance a bit indicating the particular type of message, i.e., *alarm*. However, this way to manage alarm situations may suggest the attacker to flood the communications with alarm bit set to 1. So, to avoid this scenario, we suggest to accept only a maximum number of alarm messages within a time-window, for instance $5msg/hour$[2].

5 RELATED WORK

Concerning security aspects in automotive design, the authors of (Sagstetter et al., 2013) outline the upcoming security challenges in automotive architecture design and discuss the application of a model-based design approach. This analysis was done in combination with formalized verification methods that aimed at checking and avoiding vulnerabilities already during the design process of a future automotive architectures based on Ethernet/IP.

The work in (Studnia et al., 2013) provides an overview of the protection mechanisms that could be adopted as countermeasures to identified threats.

Some solutions for automotive have been also developed. For instance, European projects such as SeVeCOM (Leinmüller et al., 2006; Wiedersheim et al., 2009; Papadimitratos et al., 2008), PRESERVE (https://www.preserve-project.eu/), and EVITA (http://www.evita-project.org/) aimed at designing secure communication architectures for internal or inter-vehicular communications. In particular, the SeVeCOM EU project (Leinmüller et al., 2006; Wiedersheim et al., 2009) developed a modular system supporting security and privacy features in V2V Ad Hoc Networks. This solution describes an architecture for integrating into the network stack a system for generating and verifying signatures based on PKI with short term key and certificates in order to guarantee the authenticity of communication partners. It is important to note that the SeVeCom system has been integrated into the network stack by inserting Inter Layer Proxies into the network stack to intercept communication messages.

Many protection mechanisms and frameworks have been developed to enforce security properties in the VANET. For instance, there are generic security mechanisms not customized for automotive but that work for any mobile ad hoc network. Some solutions for automotive have been also developed. Indeed, the US Dept. of Transport identified several application scenario where VANETs can be useful (National Highway Traffic Safety Administration and others, 2005). These applications can be categorized in safety and non-safety. Basically, the non safety are related to traffic, congestion and so on. This points out how securing VANETs is important. For this reason in (Razzaque et al., 2013), the authors provide a possible list of all possible adversaries in any security system and present also several security solutions able to cope with different issues. It is worth noticing that the main security issues of V2X communication mainly concerns security issues peculiar of WiFi connection.

The authors of (Malip et al., 2014), propose a protocol for securing communication in VANETs which exploits "certificate-less" signature. This protocol uses a reputation server, which is responsible for the distribution and management of identities and cryptographic credentials of vehicles. The main purpose is to guarantee the reliability of messages. The solution we propose is also based on a reputation system but with the aim to deal with issues related to the availability of the VANET and its services for drivers.

Further approaches listed in (Chen et al., 2011) do not require authentication to guarantee the authenticity of a broadcast announcement. These approaches take into account the number of received messages with the same warning; if this number is greater than a threshold, the announce is considered true. The security aspects they mainly consider are reliability of messages, privacy, and auditability. They do not care about availability of the VANET. Both solutions are based on an algorithm that takes as input the number of exchanged messages but our algorithm, being focused on DoS attack, considers also the source of the messages as input information and calculates the reputation of a vehicle.

In (Raya and Hubaux, 2005), the authors survey about security issues in VANET and sketches some possible solutions for some of them. For instance, in order to mitigate the DoS attacks, they propose the capability of switching between different channels or even communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them is brought down. However, this could be not feasible in case vehicles have not all the necessary technologies. The approach we propose overcomes this issue

[2] As we have already state above, also this value can be further improved after performing simulations.

by identifying the possible attacker and dropping his messages. In this way, the algorithm works as a firewall by isolating the possible malicious vehicle.

The authors of (Leinmüller et al., 2010) present a solution to protect VANET communications from roadside attackers. In this scenario, the attacker is someone located next to a road and it is a vehicle that generates messages that are not distinguishable from the other cars. In this way, the attacker is able to send fake messages on the net to influence the behaviour of drivers on the road. Even though the problem we face is similar, we focus on internal attackers, i.e., vehicles that send too much messages to reduce the availability of the VANET. Furthermore, the approach they proposed in based on the distance of the attacker while we propose an algorithm based on reputation of a vehicle.

Being more general, literature about reputation system in peer-to-peer network can be also considered. As an example, the work in (Stakhanova et al., 2004) presents a fully decentralized approach to compute the reputation of peers based on the traffic between a node and its peers, independently of these peers willingness to cooperate in calculation of their reputation. A part form the different network communication, the main difference between this work and the one we propose is the final goal: in (Stakhanova et al., 2004) they want to find the optimal peers for the communication, while we want to identify the possible attacker and prevent it to badly affect the communication among all the other nodes in the VANET.

6 CONCLUSION AND FUTURE WORK

Automotive systems present many security challenges that depend on several factors such as, the heterogeneity of embedded systems and communication technologies to make vehicle connected. In this paper we focus on Vehicle to Vehicle communication and, in particular, we provide a reputation based algorithm able to evaluate whether a vehicle behaves as an attacker. As a result we are able to verify if a DoS attack happens and mitigate it to preserve the availability of vehicle communications for safety communication.

As ongoing work, we are simulating the performance of the proposed algorithm to evaluate its efficiency and feasibility in the verification and validation of both V2V and V2X communications. In the future, we aim at enhancing our proposal to overcome other security issues, such as data integrity and confidentiality. We will refine our algorithm to prevent malicious vehicles, for instance, from sharing wrong identity information and creating messages that look like forwarded messages but are actually newly created ones. Furthermore, we would like to consider the possibility that a malicious vehicle tries to attack the infrastructure by, for instance, uploading fake observation tables to the server to arbitrarily change the reputation scores The ultimate goal will be the deeply analysis of the impact of the proposed solution on safety aspects, such as, how much we are able to improve the traffic on a road and to reduce traffic jam.

ACKNOWLEDGEMENT

Work partially supported by the H2020-MSCA-ITN-2015-NeCS 675320.

REFERENCES

Bella, G., Bistarelli, S., and Massacci, F. (2005). Retaliation: Can we live with flaws? In *WORKSHOP ON INFORMATION SECURITY ASSURANCE AND SECURITY*.

Bella, G., Costantino, G., and Riccobene, S. (2008). Managing reputation over manets. In Rak, M., Abraham, A., and Casola, V., editors, *Proccedings of the Fourth International Conference on Information Assurance and Security, IAS 2008, September 8-10, 2008, Napoli, Italy*, pages 255–260. IEEE Computer Society.

Chen, L., Ng, S.-L., and Wang, G. (2011). Threshold anonymous announcement in vanets. *Selected Areas in Communications, IEEE Journal on*, 29(3):605–615.

Chou, C.-M., Li, C.-Y., Chien, W.-M., and Lan, K.-c. (2009). A feasibility study on vehicle-to-infrastructure communication: Wifi vs. wimax. In *Mobile Data Management: Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on*, pages 397–398. IEEE.

Deng, H., Li, W., and Agrawal, D. (2002). Routing security in wireless ad hoc networks. *Communications Magazine, IEEE*, 40(10):70–75.

IET, The Institution of Engineering and Technology (2014). Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspective for connected vehicles.

Leinmüller, T., Buttyan, L., Hubaux, J.-P., Kargl, F., Kroh, R., Papadimitratos, P., Raya, M., and Schoch, E. (2006). Sevecom-secure vehicle communication. In *IST Mobile and Wireless Communication Summit*, number LCA-POSTER-2008-005.

Leinmüller, T., Schmidt, R. K., and Held, A. (2010). Cooperative position verification-defending against roadside attackers 2.0. In *Proceedings of 17th ITS World Congress*.

Malip, A., Ng, S.-L., and Li, Q. (2014). A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks. *Security and Communication Networks*, 7(3):588–601.

National Highway Traffic Safety Administration and others (2005). Vehicle safety communications project task 3 final report: Identify intelligent vehicle safety applications enabled by dsrc. *DOT HS S09 S*, 59.

Papadimitratos, P., Buttyan, L., Holczer, T. S., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., and Hubaux, J.-P. (2008). Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, 46(11):100–109.

Qian, Y. and Moayeri, N. (2008). Design of secure and application-oriented vanets. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2794–2799. IEEE.

Raya, M. and Hubaux, J.-P. (2005). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21. ACM.

Razzaque, M., Salehi, A., and Cheraghi, S. M. (2013). Security and privacy in vehicular ad-hoc networks: survey and the road ahead. In *Wireless Networks and Security*, pages 107–132. Springer.

Sagstetter, F., Lukasiewycz, M., Steinhorst, S., Wolf, M., Bouard, A., Harris, W. R., Jha, S., Peyrin, T., Poschmann, A., and Chakraborty, S. (2013). Security challenges in automotive hardware/software architecture design. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 458–463. EDA Consortium.

Stakhanova, N., Ferrero, S., Wong, J. S., and Cai, Y. (2004). A reputation-based trust management in peer-to-peer network systems. In Bader, D. A. and Khokhar, A. A., editors, *Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems, September 15-17, 2004, The Canterbury Hotel, San Francisco, California, USA*, pages 510–515. ISCA.

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., and Laarouchi, Y. (2013). Survey on security threats and protection mechanisms in embedded automotive networks. In *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on*, pages 1–12. IEEE.

Wang, C. and Thompson, J. (1997). Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network. US Patent 5,613,039.

Wiedersheim, B., Sall, M., and Reinhard, G. (2009). Sevecom—security and privacy in car2car ad hoc networks. In *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, pages 658–661. IEEE.